УДК 343.3/.7

КУЧЕРИНА С.Є., *кандидат військових наук, доцент,* провідний науковий співробітник науково-дослідної лабораторії військового права, права національної та міжнародної безпеки НДІ інформатики і права НАПрН України.
ОЛЄЙНІКОВ Д.О., *кандидат юридичних наук,* начальник відділу наукової та науково-дослідної роботи ІПЮК для СБУ НЮУ ім. Ярослава Мудрого.
ORCID: https://orcid.org/0000-0002-8515-5241.

СУЧАСНИЙ СТАН КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. *У роботі здійснено науковий аналіз сучасного стану норм кримінального права, які встановлюють кримінальну відповідальність за посягання на об'єкти критичної інфраструктури чи на їх інформаційну інфраструктуру, та оцінено їх ефективність з точки зору системності кримінально-правової охорони. Виявлено, що наразі рівень кримінально-правової охорони об'єктів критичної інфраструктури є недостатнім та безсистемним. Це обумовлено: відсутністю у законодавстві, яке встановлює кримінальну відповідальність за суспільно небезпечні діяння, індивідуалізованого підходу до критичної інфраструктури взагалі та її об'єктів зокрема; не врахуванням у кримінальному праві сучасного розвитку організаційно-правових засад критичної інфраструктури та ін. Авторами запропоновані конкретні кроки, що сприятимуть захищеності вітчизняної критичної інфраструктури кримінально-правовими засобами.*

Ключові слова: *об'єкти критичної інфраструктури, об'єкти критичної інформаційної інфраструктури, кримінальна відповідальність, кримінально-правова охорона.*

Summary. *The scientific analysis of the current state of criminal law, which establishes criminal liability for encroachment on critical infrastructure or their information infrastructure, and evaluates their effectiveness in terms of systemic criminal law protection. It is revealed that currently the level of criminal protection of critical infrastructure is insufficient and unsystematic. This is due to: the lack of legislation that establishes criminal liability for socially dangerous acts, an individualized approach to critical infrastructure in general and its facilities in particular; not taking into account in criminal law the modern development of organizational and legal principles of critical infrastructure, etc. The authors propose concrete steps that will contribute to the protection of domestic critical infrastructure by criminal law.*

Keywords: critical infrastructure facilities, critical information infrastructure facilities, criminal liability, criminal law protection.

Аннотация. *В работе осуществлен научный анализ современного состояния норм уголовного права, устанавливающих уголовную ответственность за посягательство на объекты критической инфраструктуры или на их информационную инфраструктуру, и оценена их эффективность с точки зрения системности уголовно-правовой охраны. Выявлено, что существующий уровень уголовно-правовой охраны объектов критической инфраструктуры является недостаточным и бессистемным. Это обусловлено: отсутствием в законодательстве, которое устанавливает уголовную ответственность за общественно опасные деяния, индивидуализированного подхода к критической инфраструктуры вообще и ее объектов в частности; игнорированием уголовным правом современного развития организационно-правовых основ критической инфраструктуры и др. Авторами предложены конкретные шаги, которые поспособствуют защищенности отечественной критической инфраструктуры уголовно-правовыми средствами.*

Ключевые *слова: объекты критической инфраструктуры, объекты критической информационной инфраструктуры, уголовная ответственность, уголовно-правовая охрана.*

Постановка проблеми. Реалії сьогодення переконливо демонструють удосконалення й переорієнтацію форм і методів глобального деструктивного впливу в площину кіберпростору, що дозволяє досягати більш руйнівного злочинного результату із задіянням новітніх технологій. З цього приводу О.П. Єрменчук підкреслює, що "…Україна протистоїть найсерйознішому за роки своєї незалежності виклику у сфері забезпечення державної безпеки. Військовий конфлікт на сході країни, торгівельні війни, економічна експансія, різке посилення тероризму, небувалий ріст злочинності, руйнування та пошкодження численних підприємств, у тому числі стратегічно важливих, інфраструктурних об'єктів, втрата новітніх технологій – все це та інші ризики вимагають від держави нових підходів до завчасного виявлення загроз та їх попередження і припинення" [1, с. 5]. При цьому, як зауважує О.М. Суходоля, система захисту критичної інфраструктури має будуватися виходячи з необхідності реагування на комплекс загроз та їх узгоджену реалізацію і спрямовуватися на забезпечення стійкості функціонування системи життєдіяльності суспільства, національної економіки та держави. Це завдання не може бути забезпечене лише заходами посилення фізичної охорони окремих об'єктів [2, с. 74].

Як свідчить попередній аналіз, кримінально-правова охорона критичної інфраструктури в Україні значно відстає від темпів розвитку злочинності у кіберпросторі та сфері інформаційної безпеки держави взагалі. Означена обставина, а також окремі нормотворчі ініціативи щодо об'єктів критичної інфраструктури обумовлюють необхідність активізації наукового аналізу в напрямку вироблення дієвого та сучасного механізму кримінально-правової охорони критичної інфраструктури в Україні.

Результати аналізу наукових публікацій. В принципі, наукові роботи, які досліджують ті або інші питання забезпечення безпеки об'єктів критичної інфраструктури, можна поділити на декілька напрямів:

- організаційно-правові засади забезпечення кібербезпеки об'єктів критичної інфраструктури. В зазначеному напрямі наукові розвідки здійснювали такі фахівці як В. Абрамов, В. Білоус, О. Довгань, І. Доронін, О. Насвіт, А. Пашков, А. Тарасюк, Т. Ткачук, І. Уряднікова, Л. Щаслива та інші;

- кримінально-правова охорона об'єктів критичної інфраструктури. Цей напрям досліджували Д. Пашнєв, О. Сандул, Т. Созанський, О. Суходоля, А. Таран та інші.

Наукові здобутки та висновки вказаних вчених покладено в основу дослідження, окремі положення набули подальшого розвитку. Разом з цим, динаміка соціальних, політичних та технічних перетворень в суспільстві є настільки гострою, а нормотворчі ініціативи численними, що обрана тематика навряд чи втратить свою актуальність найближчими роками.

Метою статті є аналіз сучасного стану кримінально-правової охорони об'єктів критичної інфраструктури та вироблення пропозицій щодо її удосконалення.

Виклад основного матеріалу. Рішенням Ради національної безпеки і оборони України "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури" від 29.12.16 р. введеним в дію Указом Президента України від 16.01.17 р. № 8/2017, Кабінету Міністрів України було доручено поетапно: 1) розробити за участю Національного інституту стратегічних досліджень і схвалити концепцію створення державної системи захисту критичної інфраструктури та план заходів з її

реалізації; 2) після схвалення концепції створення державної системи захисту критичної інфраструктури розробити за участю Служби безпеки України, Служби зовнішньої розвідки України і Національного банку України та внести в установленому порядку на розгляд Верховної Ради України проект Закону України "Про критичну інфраструктуру та її захист", в якому передбачити врегулювання питань, зокрема, щодо:

- створення державної системи захисту критичної інфраструктури;
- визначення органу, відповідального за координацію діяльності із захисту критичної інфраструктури в мирний час та в умовах особливого періоду;
- визначення функцій, повноважень та відповідальності центральних органів виконавчої влади та інших органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів об'єктів критичної інфраструктури;
- запровадження єдиної методології проведення оцінки загроз критичній інфраструктурі та реагування на них, зокрема щодо аварій і технічних збоїв, небезпечних природних явищ, зловмисних дій;
- запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації;
- засад державно-приватного партнерства та ресурсного забезпечення у сфері захисту критичної інфраструктури;
- міжнародного співробітництва у сфері захисту критичної інфраструктури.

Трохи менше, ніж через рік, після вказаного вище Рішення РНБО України було прийнято Закон України "Про основні засади забезпечення кібербезпеки України", в якому міститься законодавча дефініція об'єктів критичної інфраструктури. Так, відповідно до п. 16 ч. 1 ст. 1 вказаного Закону, до критично важливих об'єктів інфраструктури (об'єктів критичної інфраструктури) віднесені підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Наступний термін, який в контексті досліджуваної теми має важливе значення, визначений у п. 19 згаданої норми. Так, об'єкт критичної інформаційної інфраструктури – це комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури. Таким чином, ми маємо дворівневий об'єкт, що складається власне з об'єкта критичної інфраструктури та його комунікаційної або технологічної системи, яка є уразливою для кібератак. Іншими словами, інформаційна інфраструктура є захисною надбудовою над об'єктом критичної інфраструктури, призначення якої – захищати сам об'єкт від деструктивного впливу в кіберпросторі. О.П. Єрменчук вказує, що провідні світові держави, поряд з фізичною інфраструктурою, виділяють та здійснюють захист кіберкритичної інфраструктури [2, с. 13]. І дійсно, наприклад, у Плані захисту критичної інфраструктури США від 2015 р. закріплено, що забезпечення безпеки та стійкості фізичної та кіберкритичної інфраструктури сприяє мінімізації наслідків від дії загроз та сприяє її швидкому відновленню [3].

Механізм формування національного та секторальних переліків об'єктів критичної інформаційної інфраструктури в Україні визначається Порядком формування переліку

об'єктів критичної інформаційної інфраструктури, затвердженим постановою Кабінету Міністрів України від 9 жовтня 2020 року № 943. Зазначеним Порядком безпека об'єкта критичної інфраструктури визначається як стан захищеності об'єкта критичної інфраструктури, за якого забезпечується функціональність і безперервність його роботи та/або можливість надання ним основних послуг. Під захистом об'єктів критичної інформаційної інфраструктури розуміються організаційні, нормативно-правові, інженерно-технічні та інші заходи, спрямовані на забезпечення безпеки об'єктів критичної інформаційної інфраструктури [4].

Причини створення дворівневого об'єкта на базі об'єкта критичної інфраструктури мають свою логіку в контексті того, що "захист критичної інфраструктури поєднує три основні напрями: 1) захист від загроз у сфері державної безпеки; вони можуть включати внутрішні загрози та фізичне знищення КІ; 2) захист від кіберзагроз; 3) захист від надзвичайних ситуацій" [1, с. 14]. Враховуючи технологічні особливості окремих об'єктів критичної інфраструктури, їх власники змушені створювати технологічні системи як для управління циклом діяльності, так і з метою попередження зупинки чи руйнування об'єкта внаслідок, наприклад, помилки, техногенної аварії чи стихійного лиха. З одного боку, така ускладнена структура забезпечує захист об'єкта від зазначених вище загроз, з іншого ж боку, об'єкт стає більш уразливим за рахунок необхідності захищати також і саму інформаційну інфраструктуру.

Переходячи до суті кримінально-правової охорони, погодимось із В.В. Кузнецовим, який визнає її як, по-перше, певну систему кримінально-правових засобів, до яких слід включити кримінально-правові норми (заборонні, роз'яснювальні, заохочувальні та обмежувальні) та методи кримінально-правової політики (криміналізація та декриміналізація, пеналізація та депеналізація), за допомогою яких нормативність права переводиться в упорядкованість суспільних відносин [5, с. 109]. Чим обумовлені особливості вітчизняної кримінально-правової охорони критичної інфраструктури?

По-перше, існуючі норми розраховані, перш за все, на протидію внутрішнім загрозам, та є мало орієнтованими на сучасну динаміку та еволюцію злочинної діяльності як у кіберпросторі, так і в реальному середовищі.

По-друге, вітчизняним законодавцем так і не сформовано ефективний кримінально-правовий інститут, який би поєднував багаторівневий захист об'єктів критичної інфраструктури та їх інформаційної інфраструктури як від внутрішніх, так і від зовнішніх загроз.

Об'єкти критичної інфраструктури як окремий об'єкт злочину не розглядаються наукою кримінального права, тому їх кримінально-правова охорона здійснюється через відповідні кримінально-правові норми, які розміщені законодавцем в різних розділах Особливої частини Кримінального кодексу України (далі – КК України). Так, існуючі норми КК України в контексті кримінально-правового захисту об'єктів критичної інфраструктури встановлюють кримінальну відповідальність за:

1) умисне знищення чи пошкодження майна (ст. 194 КК України).

М.І. Мельник та М.І. Хавронюк називають основним безпосереднім об'єктом цього злочину право власності. Додатковим факультативним об'єктом, на їх думку, можуть виступати громадський порядок, екологічна безпека, життя і здоров'я людини. Що стосується предмету злочину, то ним може бути будь-яке майно як рухоме, так і нерухоме, крім окремих його видів, знищення чи пошкодження яких передбачено КК України як спеціальний вид знищення чи пошкодження майна [6, с. 531]. Ця норма є

“базовою”, оскільки виключає наявність спеціальних ознак суб’єктивної сторони складу злочину.

Проте, необхідно враховувати, що здійснення особою суспільно небезпечної діяльності, яка виразилась в посяганні на об’єкти критичної інфраструктури, в більшості випадків матиме досить специфічну мету чи мотиви. Так, якщо кінцевою метою посягання на об’єкт критичної інфраструктури є, наприклад, масове знищення рослинного або тваринного світу, отруєння атмосфери або водних ресурсів, які відбудуться внаслідок знищення такого об’єкта, вчинене додатково слід кваліфікувати за ст. 441 КК України. У разі, коли посягання на об’єкт критичної інфраструктури вчиняється в контексті надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України, то вчинене додатково має кваліфікуватись за ч. 1 ст. 111 КК України.

2) Враховуючи, що, відповідно до п. 1 ч. 1 ст. 6 Закону України “Про основні засади забезпечення кібербезпеки”, до об’єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях енергетики, умисне пошкодження або руйнування об’єктів електроенергетики, якщо ці дії призвели або могли призвести до порушення нормальної роботи цих об’єктів, або спричинили небезпеку для життя людей, може кваліфікуватись за ст. 194-1 КК України;

3) диверсію (ст. 113 КК України), в тому випадку, коли особа, яка вчинила посягання на об’єкт критичної інфраструктури, прагнула ослабити державу. При цьому автори Науково-практичного коментаря до Розділу І Особливої частини КК України відносять об’єкти, які є невід’ємними складовими національної безпеки України та мають важливе народногосподарське чи оборонне значення, до предмету диверсії [7, с. 140]. Погоджуючись із означеною точкою зору, зауважимо, що, за відсутності мети ослабити державу та наявності іншої мети кримінально-правова оцінка посягання на сам об’єкт критичної інфраструктури буде іншою;

4) терористичний акт (ст. 258 КК України), якщо посягання на об’єкт критичної інфраструктури було вчинено з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, міжнародними організаціями, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста).

В контексті розглядуваного злочину необхідно згадати про термін “кібертероризм”, який введено Законом України “Про основні засади забезпечення кібербезпеки України”. Кібертероризм вважають одним із видів технологічного тероризму – злочинів, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров’я людей речовин, засобів електромагнітної дії, комп’ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об’єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру [8, с. 21]. Разом з цим в КК України відсутні спеціальні норми (чи частини статей), які б виділяли кібертероризм в окремий склад злочину;

5) напад на об'єкти, на яких є предмети, що становлять підвищену небезпеку для оточення (ст. 261 КК України) – напад на об'єкти, на яких виготовляються, зберігаються, використовуються або якими транспортуються радіоактивні, хімічні, біологічні чи вибухонебезпечні матеріали, речовини, предмети, з метою захоплення, пошкодження або знищення цих об'єктів;

6) пошкодження шляхів сполучення і транспортних засобів (ст. 277 КК України) ядерної енергетики [9, с. 62].

В принципі, наведений перелік варіантів кримінально-правової оцінки суспільно небезпечних діянь, пов'язаних із посяганнями на об'єкти критичної інфраструктури, не є вичерпним, та, в залежності від конкретних ситуацій, може бути продовжений в багатьох напрямках. Означена обставина чітко вказує на розпорошеність відповідних норм, які можуть бути застосовані як засіб кримінально-правової охорони об'єктів критичної інфраструктури. Причина цього, як вказувалось вище, полягає в тому, що об'єкти критичної інфраструктури не розглядаються наукою кримінального права як окремі об'єкти злочину.

Що стосується спеціальної кримінально-правової охорони критичної інформаційної інфраструктури, то на її необхідності, "зважаючи на зростання негативних наслідків для держави, які завдаються кібератаками на інформаційну інфраструктуру органів державної влади, та на можливу шкоду, пов'язану з можливими кібератаками на промислові та інші об'єкти критичної інфраструктури, їх підвищену суспільну небезпечність" [10, с. 75], свого часу наголошував Д.В. Пашнєв.

У вітчизняному законодавстві містяться нереалізовані спроби впровадження кримінальної відповідальності за посягання на критичну інформаційну інфраструктуру. Так, Законом України "Про внесення змін до Закону України "Про судоустрій і статус суддів" та процесуальних законів щодо додаткових заходів захисту безпеки громадян" від 16.01.14 р. № 721-VII [11] були криміналізовані:

- несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури (ст. 361-3 КК України);

- несанкціоновані збут або розповсюдження інформації з обмеженим доступом, що оброблюється в державних електронних інформаційних ресурсах (ст. 361-4 КК України);

- несанкціоновані дії з інформацією, що оброблюється в державних електронних інформаційних ресурсах або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах критичних об'єктів національної інформаційної інфраструктури, вчинені особою, яка має право доступу до такої інформації (ст. 362-1 КК України).

Наведені вище норми так і не стали підґрунтям до кримінально-правової охорони критичної інформаційної інфраструктури, оскільки Закон України від 16.01.14 р. № 721-VII втратив чинність на підставі Закону України "Про визнання такими, що втратили чинність, деяких законів України" від 28.01.14 р. № 732-VII [12]. Разом з цим, навіть і з цих норм кримінально-правова охорона критичної інформаційної інфраструктури встановлювалась фактично лише ст. 361-3 КК України. Вказана норма передбачала кримінальну відповідальність за суспільно небезпечне діяння, яке виразилось в несанкціонованому втручанні в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем критичних об'єктів національної інформаційної інфраструктури, що призвело до витоку,

втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації.

Разом з цим, наприклад, в КК РФ передбачена кримінальна відповідальність за неправомірний вплив на критичну інформаційну структуру РФ (ст. 274.1), до якої може бути притягнуто особу за:

- створення, розповсюдження і (чи) використання комп'ютерних програм чи іншої комп'ютерної інформації, завідомо призначених для неправомірного впливу на критичну інформаційну інфраструктуру РФ, у тому числі для знищення, блокування, модифікації, копіювання інформація, яка в ній міститься, чи нейтралізації засобів захисту вказаної інформації;

- неправомірний доступ до охоронюваної комп'ютерної інформації, яка міститься в критичній інформаційній інфраструктурі РФ, у тому числі з використанням комп'ютерних програм чи іншої комп'ютерної інформації, які завідомо призначені для неправомірного впливу на критичну інформаційну інфраструктуру РФ, чи інших шкідливих комп'ютерних програм, якщо він призвів до завдання шкоди критичній інформаційній інфраструктурі РФ;

- порушення правил експлуатації засобів зберігання, обробки чи передачі охоронюваної комп'ютерної інформації, що міститься в критичній інформаційній інфраструктурі РФ, чи інформаційних систем, інформаційно-телекомунікаційних мереж, автоматизованих систем управління, мереж електрозв'язку, що відносяться до критичної інформаційної інфраструктури РФ, або правил доступу до вказаних інформації, інформаційних систем, інформаційно-телекомунікаційних мереж автоматизованих систем управління, мереж електрозв'язку, якщо це призвело до завдання шкоди критичній інформаційній інфраструктурі РФ [13].

Наразі ж перераховані вище дії, що розцінюються як неправомірний вплив на критичну інформаційну інфраструктуру, в вітчизняному законодавстві можуть бути кваліфіковані за відповідною нормою, яка міститься в Розділі XVI КК України (Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку). В цьому контексті вважаємо абсолютно доцільним погодитись із окремими висновками Д.П. Пашнєва, які він зробив ще в 2014 році. Так, вказаний учений підкреслював, що зміст статей, які призвані охороняти інформаційно-телекомунікаційні системи від суспільно небезпечних посягань (ст. 361 – 363-1 КК України), суперечить підходу іноземних країн до кримінально-правової охорони державних інформаційних ресурсів, оскільки державні інформаційно-телекомунікаційні системи та інформаційні ресурси є лише окремим видом предмету складів цих злочинів, поряд з іншими, посягання на які мають значно нижчий ступінь суспільної небезпечності. Це не дозволяє виокремити особливості суспільно небезпечних діянь, вчинених з використанням комп'ютерних технологій проти інформаційно-телекомунікаційних систем державного та суспільного значення, індивідуалізувати відповідальність осіб, які їх вчинили [10, с. 79].

О.В. Таран і О.Г. Сандул, проаналізувавши стан кримінально-правової охорони об'єктів критичної інфраструктури в ядерній енергетиці, зауважили, що, "зважаючи на те, що наразі тільки відбувається формування спеціального законодавства, триває створення переліку об'єктів критичної інфраструктури, доцільно говорити про перспективи удосконалення КК України" [9, с. 65]. Такі удосконалення, на думку згаданих фахівців, мають полягати у "запровадженні окремої норми (норм), якою буде передбачено кримінальну відповідальність за посягання на об'єкти критичної інфраструктури. На теперішній час кримінально-правовою охороною охоплюється лише

частина таких об’єктів. Звичайно, у кримінально-правовій нормі не доцільно передбачати увесь перелік об’єктів критичної інфраструктури, адже по-перше, він значний за обсягом, а по-друге, зміни і доповнення до цього переліку, які будуть вноситись за результатами його періодичного перегляду, потребуватимуть відповідних змін до КК України. Тому диспозиція правової норми очевидно матиме бланкетний характер. У чинному КК України відповідні норми розміщені у різних його розділах, а отже мають різний родовий об’єкт, що не відповідає загальній концепції критичної інфраструктури. Отже, доповнення існуючих правових норм відповідними частинами з метою диференціації кримінальної відповідальності за такі злочини не вирішить зазначених проблем. Тому відповідну норму (норми) потрібно передбачити у Розділі І Особливої частини КК “Злочини проти основ національної безпеки України” [9, с. 65].

Можемо погодитись із висновками О.В. Тарана і О.Г. Сандула в частині того, що відсутність єдиного родового об’єкта не відповідає загальній концепції критичної інфраструктури. Одночасно заперечимо доцільність впровадження кримінальної відповідальності за посягання на об’єкт критичної інфраструктури (чи критичної інформаційної інфраструктури) у Розділі І Особливої частини КК України “Злочини проти основ національної безпеки України”, оскільки така норма буде спеціальною по відношенню до ст. 113 КК України, що навряд чи вирішить саму проблему в цілому.

Висновки та пропозиції.

Результати наукового аналізу свідчать про те, що рівень кримінально-правової охорони об’єктів критичної інфраструктури наразі є недостатнім та безсистемним. До основних недоліків відноситься: 1) у законодавстві, яке встановлює кримінальну відповідальність за суспільно небезпечні діяння, відсутній індивідуалізований підхід до критичної інфраструктури взагалі та її об’єктів зокрема. Як було доведено, кримінально-правова охорона об’єктів критичної інфраструктури здійснюється лише в контексті кримінально-правової охорони інших об’єктів більш загального характеру (власність, громадська безпека, економічна безпека і т.п.), а самі об’єкти розглядаються на рівні предмета злочину; 2) наразі посягання на об’єкт критичної інфраструктури, яке вчиняється у кіберпросторі шляхом втручання в інформаційну інфраструктуру, розглядається як сукупність злочинів, хоча, і це цілком очевидно, вони співвідносяться як суспільно небезпечне діяння та спосіб його вчинення. Означене досить яскраво вказує на спорадичність кримінально-правової охорони об’єктів критичної інфраструктури та в подальшому може призвести до формування неоднорідної слідчо-судової практики з цих питань; 3) законодавство про кримінальну відповідальність не враховує сучасний розвиток організаційно-правових засад критичної інфраструктури, внаслідок чого втрачає здатність повною мірою охороняти інтереси держави і суспільства, які реалізуються через можливості критичної інфраструктури.

Враховуючи наведене вище, вважаємо, що в першу чергу необхідно переглянути перелік загальних об’єктів кримінально-правової охорони, передбачений ст. 1 КК України, та визначити за вертикаллю роль і місце критичної інфраструктури на рівні, наприклад, видового об’єкту, а конкретних об’єктів критичної інфраструктури – безпосереднього. В залежності від виду родового об’єкту, до якого критична інфраструктура увійде як видовий об’єкт, надалі потрібно впровадити норму про кримінальну відповідальність за посягання на об’єкт критичної інфраструктури. Також, за необхідності доцільно передбачити в статтях інших розділів КК України (наприклад, ст. 194, 258 і т.і.) посягання на об’єкт критичної інфраструктури в якості кваліфікуючої обставини, яка обтяжує покарання.

Ці та подальші кроки, на нашу думку, безперечно, сприятимуть захищеності вітчизняної критичної інфраструктури кримінально-правовими засобами та нададуть можливість в подальшому зрушити з місця застарілі нормативно-правові конструкції законодавства про кримінальну відповідальність.

Використана література

1. Єрменчук О.П. Основні підходи до орґанізації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

2. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети*. 2016. № 3. С. 62-76.

3. National Critical Infrastructure Security and Resilience Research and Development Plan, 2015. URL: https://www.dhs.gov/publication

4. Порядок формування переліку об'єктів критичної інформаційної інфраструктури, затверджений постановою Кабінету Міністрів України від 9.10.20 р. № 943URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

5. Кузнецов В. В. Кримінально-правова охорона: проблеми визначення поняття. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2015. Вип. 30(2). С. 107-110.

6. Науково-практичний коментар Кримінального кодексу України ; за ред. М.І. Мельника, М.І. Хавронюка. 7-ме вид., переробл. та допов. Київ: Юридична думка, 2010. 1288 с.

7. Сичевський В.В., Харитонов Є.І., Олєйніков Д.О. Науково-практичний коментар до Розділу І Особливої частини Кримінального кодексу України (Злочини проти основ національної безпеки України). Харьків: Право, 2016. 232 с.

8. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України"; станом на 1.01.19 р. / М.В. Гуцалюк та ін. ; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

9. Таран О.В. Сандул О.Г. Проблеми кримінальної відповідальності за посягання на об'єкти критичної інфраструктури в ядерній енергетиці. *Ядерна та радіаційна безпека*. 2019. Вип. 3. С. 58-67.

10. Пашнєв Д.В. Необхідність спеціальної кримінально-правової охорони критичної інформаційної. *Вісник Кримінологічної асоціації України*. 2014. № 6. С. 73-82.

11. Про внесення змін до Закону України "Про судоустрій і статус суддів" та процесуальних законів щодо додаткових заходів захисту безпеки громадян: Закон України від 16.01.14 р. № 721-VII. *Голос України*. № 10. (21.01.2014 р.). URL: https://zakon.rada.gov.ua/laws/show/721-18#Text

12. Про визнання такими, що втратили чинність, деяких законів України: Закон України від 28.01.14 р. № 732-VII. *Голос України*. № 19. (01.02.2014 р.). URL: https://zakon.rada.gov.ua/laws/show/732-18#Text

13. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 27.10.2020 г.). URL: http://www.consultant.ru/document/cons_doc_LAW_10699

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~